

### **Remarks**

Claims 1-9, 13-21, and 25-33 are pending but stand rejected. Claims 1-7, 13-19, and 25-31 have been amended. Claims 10-12, 22-24, and 34-36 have been cancelled. In view of the amendments and following remarks, the applicants respectfully ask for the Examiner's thoughtful reconsideration.

### **AMENDMENTS**

Each independent claim has been amended to recite (a) issuing a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain, and (b) authorizing a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used by the client computer to encrypt the print job. These amendments find support in the specification. In particular, page 4, lines 25-24 provides:

In some further embodiments of the invention, the user authenticates identity to the printer by using a security or encryption key, which the printer uses to confirm identity and authorization for users. The security key is in some embodiments issued and managed by a security module within the printer, as is described in the copending patent application titled "Printer Security Key Management", filed which is hereby incorporated by reference. The security key issued to each user in such an embodiment of the invention is therefore usable not only to ensure secure communication of data between the user and a printer, but to authenticate the user's identity to the printer for granting access to printer resources.

As stated, the issued security key is useable to authenticate the user's identity to the printer for granting access to printer resources. In short, the security key is indicative of the printer resources available to a client computer.

Furthermore, page 5, lines 8-11 describe that the printer grants certain predetermined printing resource authorization based on a policy domain determination. This authorization is granted by creating a security key that is associated with a client computer and issuing that security key to the client

computer. Page 6, lines 15-23 describe that using an issued security key, a client device can encrypt a print job to be sent to the printer. By being able to decrypt the print job, the printer can determine the client's resource authorization – that is – the authorization of the client to utilize various resources of the printer as indicated by the particular security key used to encrypt the print job.

***CLAIM REJECTIONS – 35 USC §102***

Claims 1-3, 6, 13-15, 18, 25-27, and 30 were rejected under 35 U.S.C. §102 as being anticipated by US Pub 6,952,280 issued to Tanimoto.

**Claim 1**, as amended, is directed to a printer access control module within a printer that is operable to:

1. receive a request from a client computer for printing resource authorization;
2. determine the policy domain of the requesting client computer;
3. issue a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain; and
4. authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used to encrypt the print job.

Tanimoto, as admitted by the Examiner, does not teach the use of security keys. Addressing other claims reciting the use of security keys, the Examiner cites USPN 6,711,677 issued to Wiegley. Wiegley, col. 3, line 62 through col. 5, line 24 describes a system in which a client requests a secure printing session with a printer. In response, the printer generates a session identifier and sends the session identifier along with an encryption key to the client. Once the client authenticates the transmission from the printer, the client generates a session key. The client encrypts the session key with the printer's encryption key and sends the encrypted session key and the session identifier to the printer. The

session identifier is sent to the printer in a manner that ties the session identifier to the print job. The print job is encrypted with the session key and sent to the printer. The printer can then decrypt the session key with its own private key to ensure that the session identifier has been changed from the identifier the printer sent to the client. Assuming there is no change, the printer can conclude that the print job is valid and then decrypt and print the print job.

Wiegley mentions nothing of a security key that is indicative of one or more printer resources available to client computers of the determined policy domain. Wiegley's session key is indicative only of a communication session between a client and a printer.

Consequently, neither Wiegley nor Tanimoto teaches or suggests (a) issuing a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain; and (b) authorizing a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used to encrypt the print job. For at least these reasons Claim 1 and Claims 2-9 which depend from Claim 1 are patentable over the cited art.

**Claim 13**, as amended, is directed to a printer that is operable to:

1. receive a request from a client computer for printing resource authorization;
2. determine the policy domain of the requesting client computer;
3. issue a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain; and
4. authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used to encrypt the print job.

As with Claim 1, neither Wiegley nor Tanimoto teaches or suggests (a)

issuing a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain; and (b) authorizing a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used to encrypt the print job. For at least the same reasons Claim 1 is patentable, so are Claim 13 and Claims 14-21 which depend from Claim 13.

**Claim 25**, as amended, is directed to a machine-readable medium with instructions stored thereon, the instructions when executed on a computerized system operable to cause the system to:

1. receive a request from a client computer for printing resource authorization;
2. determine the policy domain of the requesting client computer;
3. issue a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain; and
4. authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used to encrypt the print job.

As with Claim 1, neither Wiegley nor Tanimoto teaches or suggests (a) issuing a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain; and (b) authorizing a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used to encrypt the print job. For at least the same reasons Claim 1 is patentable, so are Claim 25 and Claims 26-33 which depend from Claim 25.

#### ***CLAIM REJECTIONS – 35 USC §103***

**Claims 4, 16, and 28** were rejected under 35 U.S.C. §103 as being unpatentable over US Pub 6,952,280 issued to Tanimoto in view of US Pub 2003/0151760 to Berndt. Claims 4, 16, and 25 depend from Claims 1, 13, and 25 respectively. For at least the same reasons Claims 1, 13, and 25 are patentable so are Claims 4, 16, and 25.

**Claims 5, 7, 17, 19, 29, and 31** were rejected under 35 U.S.C. §103 as being unpatentable over US Pub 6,952,280 issued to Tanimoto in view of USPN 6,985,244 issued to Bhogal. Claims 5 and 7 depend from Claim 1. Claims 17 and 19 depend from Claim 13. Claims 29 and 31 depend from Claim 25. For at least the same reasons Claims 1, 13, and 25 are patentable so are Claims 5, 7, 17, 19, 29, and 31.

**Claims 8, 9, 20, 21, 32, and 33** were rejected under 35 U.S.C. §103 as being unpatentable over US Pub 6,952,280 issued to Tanimoto in view of USPN 6,545,767 issued to Kuroyanagi . Claims 8 and 9 depend from Claim 1. Claims 20 and 21 depend from Claim 13. Claims 32 and 33 depend from Claim 25. For at least the same reasons Claims 1, 13, and 25 are patentable so are Claims 5, 8, 9, 20, 21, 32, and 33.

**Claims 10-12, 22-24, and 34-36** were rejected under 35 U.S.C. §103 as being unpatentable over US Pub 6,952,280 issued to Tanimoto in view of USPN 6,711,677 issued to Wiegley. Claims 10-12, 22-24, and 34-36 have been cancelled.

**Conclusion**

In view of the foregoing remarks and amendments, Applicant respectfully submits that Claims 1-9, 13-21, and 25-33 define allowable subject matter. The Examiner is requested to indicate the allowability of all claims in the application and to pass the application to issue.

Respectfully submitted,  
Curtis Reese

By /Jack H. McKinney/  
Jack H. McKinney  
Reg. No. 45,685

September 18, 2007